중첩 VLAN구현을 위한 확장 FDB적용 알고리즘 제안

황인섭*, 공휘식 ·

*관동대학교 전자통신공학

Extended FDB Application Algorithm Proposal for Overlap VLAN Implementation

In-sub Hwang* · Whue-sik Kong

Dept. of Electronic Communication Engineering Kwandong University

E-mail : inseub@orgio.net, kws32@mail.kwandong.ac.kr

요 약

보안과 Broadcast로 인한 성능 저하는 LAN에서 다루어야 할 가장 중요한 부분이다. Virtual LAN은 논리적으로 네트워크 그룹을 형성하여 관리하는 방법으로 LAN의 성능저하를 개선 할 수 있다.

본 연구에서 제안하는 MAC Address VLAN 알고리즘은 FDB에 확장 VID 필드와 VID 연결 범위 테이블을 추가하여 VLAN에 중첩 특성을 부여하고, 중첩 범위를 동적으로 관리한다. 이 제안 알고리즘을 적용한 VLAN은 추가적인 장비 없이 네트워크 상의 정보와 자원을 공유 할 수 있다. 본 알고리즘은 Layer 2 기능을 수행하는 스위치나 브리지에 적용이 가능하다.

ABSTRACT

Security and degradation by broadcast is the most important part that must handle in LAN. Virtual LAN can improve LAN's degradation by method to form and manages network group logically.

MAC Address VLAN algorithm that propose in this research give overlap special quality to VLAN adding extension VID field and VID connection extent table to FDB, manage overlap extent dynamically. VLAN that apply this proposal algorithm can share information and resource in network without additional equipment. Application is possible switch or Bridge that this algorithm achieves Layer 2 functions.

키워드

Virtual LAN, vlan, MAC address, VID, 이더넷

Ⅰ. 서 론

기업체나 학교 등에서 운영되고 있는 LAN은 매체 공유 특성을 지니고 있다. 최근 들어 업무의 전산화, 정보화로 인하여 LAN station의 수가 급격히 증가하고 있으며, 이에 따른 데이터 량의 증가와 보안 및 보호는 매우 중요한 문제로 대두되고 있다. [1]

LAN의 브로드캐스트 패킷은 성능 저하의 가장 큰 원인으로 작용하고 있다. VLAN(Virtual LAN) 기법은 브로드캐스트 패킷을 제한하여 LAN의 효율을 증가시키고, 아울러 보안과 보호 기능을 도모하고 있다. VLAN은 IEEE 802.1Q에 표준안이 제시되어 있으며 점차 적용 범위가 확대되고 있다.

본 연구는 MAC Address VLAN에서 VLAN의 확장과 축소를 위해 VID 연결 범위 테이블을 추가하고, 확장된 영역을 나타내기 위해 C_VID필드를 추가하였다. 이를 통해 연결 범위를 동적으로 변화시킬 수 있어 서로 다른 VLAN 사이의 연결을 가능하게 하는 알고리즘을 제안한다.

제안한 알고리즘은 2계층 기능을 수행하는 스위치 허브나 브리지에 적용하여 VLAN System을 구성할 수 있다.

II. VLAN의 기능 및 기법

2.1 VLAN의 기능과 적용

VLAN기술은 여러 가지 네트워크 장비를 활용하여 네트워크를 물리적으로 구분하는 전형적인 구조와는 달리 네트워크 관리자가 LAN 스위치를 이용하여 네트워크를 논리적으로 분할하는 기법이다.

논리적으로 분할한다는 것은 조직 구성이나, 서비스의 특성에 따라 그룹화 하는 것을 말한다. 조직 구성에 따른 그룹화는 회계, 판매, 기술 등과 같은 기능적 작업 단위에 기초하여 그룹화 하는 것을 말한다. 서비스에 따른 그룹화는 개인적인 사용자가 서버나 응용 프로그램에 따라 그룹화 하는 것을 말한다.

이와 같이 VLAN은 네트워크 특성에 따라 효율적인 디자인을 가능하게 한다.

2.2 VLAN 기법

2.2.1 Layer 1 VLAN

Layer 1 VLAN은 물리계층을 활용하는 가장 간단한 기법으로 VLAN 구성이 LAN 스위치의 물리적 포트 그룹으로 이루어진다. 사용자들은 물리적으로 연결된 스위치 포트에 기초하여 VLAN을 할당받는다.

이 기법은 포트 스위칭 기능을 사용하여 수 개의 VLAN을 구성하고, 보안성을 향상시킬 수 있으나 사용자 이동성을 지원하지 않는 단점이 있다. [2]

2.2.2 Layer 2 VLAN

Layer 2 VLAN은 OSI 7 Layer중 data link layer의 기능을 적용한 것으로 MAC Address와 프로토콜 기반 VLAN이 있다. MAC Address VLAN은 MAC Address 집합에 따라 VLAN이 형성된다. MAC address VLAN은 이동성을 지원하기 때문에 네트워크 상의 물리적인 장소에 관계없이 VLAN그룹을 유지 할 수 있다. 또한 두 개의 VLAN에 동시에 소속되어 통신을 할 수 있다.[3]

Layer 2의 LLC(Logical Link Control)을 사용하는 프로토콜 기반 VLAN은 프레임 내의 특정 필드를 지정하여 사용하기 때문에 사용자는 매체나 프레임 포맷에 투명하게 통신할 수 있다.

2.2.3 Layer 3 VLAN

Layer 3 VLAN은 network layer 프로토콜을 적용하는 것으로 서브네트 주소를 사용한다. Layer 3 VLAN은 초기 설정이 쉽고 물리적 이동에 유연하게 대응 할 수 있으나 프레임 안의 네트워크 주소를 검사하는 하는데 많은 시간이 소비된다는 문제점이 있다.[4]

III. MAC address VLAN

대부분의 LAN은 Ethernet으로 구현되어 있으며 크게 공유 LAN과 스위칭 LAN으로 구분 할 수 있다. 공유 LAN은 해당 세그먼트의 대역폭을 모든 컴퓨터들이 공유하는 네트워크이며, 스위칭 LAN은 스위치의 각각의 포트마다 전용 대역폭을 할당하여 스위칭 기법으로 네트워크를 구성하는 것이다. MAC address VLAN의 설명을 위해 스위칭 LAN으로 네트워크를 그림 1과 같이 구성하였다.

그림 1에서 WAN과 연결된 S1 스위치는 모든 포트에서 다수의 MAC address를 할당할 수 있는 Work group 스위치이다. S2, S3, S4 스위치는 S1과 연결된 port를 제외한 모든 포트가 하나의 MAC address만을 지원하는 Desk top 스위치이다. 그림 1의 모든 스위치는 Layer 2 프로토콜을 사용하는 스위치로 VLAN Aware 스위치라 한다. 각 스위치에 연결된 end-station들의 MAC address를 임의로 A1, A2 A3, A4, B1, B2. B3, B4, C1, C2, C3, C4라 하였다.

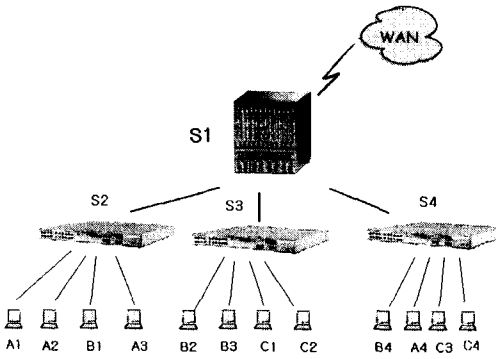

그림 1 물리적 네트워크 구성

3.1 일반적인 MAC address VLAN

MAC address VLAN의 FDB(Filtering Database)는 MAC address, VID, 포트주소 list에 의해 구성된다. FDB의 의한 VLAN 그룹화는 관리자에 의해 관리되며 임의로 변경될 수 없다. 단지 VLAN의 FDB 등록은 시스템 특성에 따라 정적이거나 동적으로 이루어진다.[5]

표1 업무특성에 따른 구성

MAC address	VID
A1, A2, A3, A4	영업
B1, B2, B3, B4	관리
C1, C2, C3, C4	생산

MAC address VLAN 스위치는 임의의 포트로 입력되는 프레임에 대해 FDB를 검색하여 프레임의 중계 여부를 결정한다.
그림 1에서 업무특성에 따라 영업, 관리, 생산 VLAN 이 표1과 같이 나누어진다면 이에 따른 VLAN의 논리적 구성은 그림 2와 같이 될 것이다

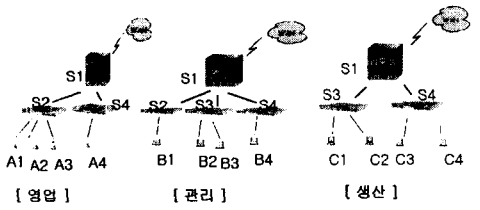

그림 2 VLAN의 구성

다시 말하면 물리적인 네트워크는 그림 1과 같이 구성되지만 논리적으로는 MAC address에 따라서 그림 2와 같이 분리된다.
MAC Address VLAN은 네트워크 자원의 이동에 대해 유연하게 대처 할 수 있으나 네트워크 내에 end-station 수가 많을 경우 초기 설정 작업이 방대하며, 네트워크 변화에 따른 관리가 복잡하다. 또한 VLAN과 VLAN 사이의 연결을 위해 고가의 3 계층 스위치 장비나 라우터를 사용해야 하는 단점이 있다.
본 연구에서 제안하는 MAC address VLAN 알고리즘은 VLAN의 확장과 축소의 동적인 변화를 위해 F_VID 연결 범위 테이블을 FDB에 추가하고, 확장된 영역을 표시하기 위해 C_VID 필드를 FDB 테이블에 추가하였다. F_VID 연결 범위 테이블에는 C_VID의 확장범위와 권한을 설정하고, 그 확장된 범위는 FDB 테이블의 C_VID에 설정된다. 제안 알고리즘은 시스템의 특정한 조건이나 노드의 네트워크 연결 상태에 따라 동적으로 VLAN 범위를 조절할 수 있어 서로 다른 VLAN 사이에 정보와 자원의 공유를 가능하게 한다.

Ⅳ. 중첩 VLAN 알고리즘 제안

4.1 알고리즘 구현을 위한 제한
그림1의 네트워크에서 VLAN 그룹화를 위한 환경 설정은 다음과 같이 결정한다.

① VID는 VLAN 그룹을 나타낸다.
② 초초 네트워크에 존재하는 모든 end-station의 FDB는 관리자가 설정한다.
③ VLAN 중첩의 범위와 권한을 결정하는 F_VID 연결 범위 테이블을 제안 알고리즘의 구현을 위해 추가한다.
④ 제안 알고리즘의 구현을 위해 FDB에 C_VID (Changed VID) 필드를 삽입하고, C_VID 필드에서 중첩의 범위를 결정한다.
⑤ C_VID 필드는 동적으로 관리된다.
⑥ C_VID는 관리자에 의해 설정된 조건에서만 변화된다.

4.2 Filtering Database
4.2.1 F_VID 연결 범위 테이블
그림 1 에서 VLAN이 영업, 관리, 생산으로 구분 되어있다면 표 2와 같은 F_VID 연결 범위 구성 테이블을 구성할 수 있다.

표 2 F_VID 연결 범위 테이블

VID	등급	연결 범위
관리	Ⅰ	영업, 생산
영업	Ⅲ	생산
생산	Ⅱ	

표2의 F_VID 필드는 MAC address에 할당되는 VLAN 구분을 위한 그룹 ID이다. 등급 필드는 해당 F_VID의 보안 관리 등급이다. 등급Ⅰ는 F_VID의 연결 범위가 VLAN 구축시 초기화 된 값이며, 등급Ⅱ는 관리자에 의해서만 F_VID의 연결 범위를 변경할 수 있고, 등급Ⅲ는 프로그램에 의해 F_VID의 연결 범위가 바뀔 수 있음을 의미한다. 연결 범위 필드는 해당 F_VID와 연결 가능한 타 VLAN F_VID들을 나타낸다. 예를 들면 표2에서 관리 VLAN의 Broadcast 영역은 다른 VLAN 전체를 포함 할 수 있음을 의미한다. 또한 영업의 Broadcast 영역은 VLAN 그룹 '생산'의 영역을 포함한다.

4.2.2 Desk top VLAN 스위치의 FDB
표3의 MAC Address 필드는 16진수로 station들의 MAC Address를 나타낸다. F_VID 필드는 MAC Address에 부여된 최초의 VID이고, C_VID 필드는 F_VID와 F_VID 연결 범위 테이블을 참조하여 연결의 범위가 확장된 VID를 나타낸다. Port 필드는 현재 스위치에 연결된 MAC address에 대한 물리적인 주소이다

표3 Filtering Database 테이블

Mac Address	F_VID	C_VID	Port
A1-32-5D-4D-B4-E2	관리	영업	1
C1-3F-4D-98-FF-42	영업	생산	2
CD-65-F4-B6-4C-2A	생산		3
1F-D4-F8-6D-D4-2C	영업		4
FF-3A-8C-4F-CD-7D	관리	생산	
C6-8A-6D-CD-F4-FF	관리		6

4.2.3 접속 상태 테이블
표4의 MAC address 필드는 표3에 등록된 MAC

address중 F_VID 등급이 Ⅲ에 해당하는 MAC address를 가진 End-station의 연결 상태를 저장하는 테이블이다. F_VID 필드는 목적지 MAC address의 F_VID이고, 나머지 최종접속일, 접속횟수 필드는 네트워크 작업 정도를 알 수 있는 데이터들이다.

표4 접속 상태 테이블

MAC address	F_VID	최종 접속일	접속 횟수
A1-32-5D-4D-B4-E2	생산	00.10.01	50
C1-3F-4D-98-FF-42	관리	01.05.31	68
CD-65-F4-B6-4C-2A	영업	00.12.15	31

4.2.4 Work group 스위치 VLAN의 FDB

표5의 MAC address 필드는 네트워크 내에 등록된 모든 노드에 대한 MAC address를 포함한다. Work group스위치의 FDB는 Desk top스위치의 FDB 추가, 갱신에 따라 동시에 업데이트된다.

Work group스위치 FDB는 C_VID의 변경을 수행하지 않으며 프레임의 중계를 위한 Filtering 작업만 수행한다.

표 5 Work group FDB 테이블

Mac Address	F_VID	C_VID	Port
A1-32-5D-4D-B4-E2	관리	영업	1
C1-3F-4D-98-FF-42	생산		1
CD-65-F4-B6-4C-2A	영업	생산	1
1F-D4-F8-6D-D4-2C	관리		2
FF-3A-8C-4F-CD-7D	영업	생산	2
...		...	...
41-FF-5D-8D-FA-42	관리	영업	3

4.3 C_VID의 동적 관리 알고리즘

Desktop 스위치에서 이루어지는 C_VID의 동적인 변화는 VLAN 범위의 확장과 축소를 결정한다. 즉 C_VID의 동적인 변화에 의해 서로 다른 VLAN 사이에 연결이 가능하게 된다. C_VID의 변화는 다음과 같은 순서에 의해 이루어진다.

스위치는 입력되는 프레임에서 F_VID를 확인하고, F_VID의 관리 등급이 Ⅲ이면 표2의 연결범위 테이블을 검색하여 VLAN의 통신 그룹의 확대여부를 결정한다. 이 결과에 따라서 접속 상태 테이블인 표4를 갱신한다. 표4는 표3의 C_VID를 동적으로 변화시키는 기초 자료가 된다. C_VID는 네트워크 특성에 맞게 조절된 시점에 따라 표2의 F_VID 연결 범위 테이블과 표4의 접속 상태 테이블을 참조하여 변경된다. 이때 표5의 FDB 테이블도 갱신된다. 이에 따른 자세한 알고리즘을 PesudoCode로 나타내면 아래와 같다.

F : Frame
SMA : source MAC address
DMA : destination MAC address
T1 : 표2의 F_VID 연결 범위 테이블
T2 : 표3의 Desk top FDB 테이블
T3 : 표4의 접속 상태 테이블
T4 : 표5의 Work group FDB 테이블

① Desk top 스위치에 프레임이 입력될 때

```
F 수신 ;
if ( SMA가 T2에 있는가 ? )
   if( DMA가 Broadcast 인가 ? )
   {  T2에서 SMA에 따른 F_VID 확인;
      F_VID에 따른 VLAN으로 F 송신;
      T1에서 F_VID의 연결범위 확인 ;
      확장 가능한 VLAN 그룹으로 F 송신;
      상위 스위치로 F 송신;
    }
   else if( DMA가 T2에 존재하는가?)
         /* Broadcast아니고, DAM 존재  */
      if (SMA에 해당 F_VID등급 =='Ⅲ' ?)
       {    T3에 데이터 레코드 추가;
            if (C_VID 변경 확인 시점인가 ? )
              { T1에서 F_VID의 확장범위확인;
                T3에서 연결 상태를 확인;
                C_VID 확장 Or 축소;
               }
            DMA로 F 전송;
       }
   else
        상위 스위치로 F전송;
else
   F  discard;
```

② Work group 스위치에 프레임이 수신 될 때

```
F 수신;
if ( F 수신 Port 주소가 LAN인가 ?)
    SMA의 VID 해당 Port로 F 송신 ;
  else  /* 외부(WAN)에서 입력된 F이면*/
    if ( Broadcast F 이면 ?)
       모든 포트로 프레임 송인;
    else
        DMA가 속한 Port F 송신;
```

4.5 알고리즘 적용 스위치의 프레임 중계

일반적인 MAC address VLAN을 적용한 스위치의 중계 테이블은 표6과 같고, 제안 알고리즘을 적용한 스위치의 중계 테이블은 표7과 같다.

표6과 표7에서 SA는 송신지 주소, DA는 수신지 주소, 종류는 통신 가능 여부를 나타낸다. 통신은 B(Broadcast), D(Discard), R(Reply)로 표현하고, S1, S2, S3, S4는 스위치의 중계여부를 나타낸다.

표6에서 서로 다른 VLAN에 속한 노드들이 스위치를 통해 연결이 될 수 없음을 볼 수 있다. 하지만 제안 알고리즘을 적용한 표7에서는 F_VID

연결 범위 내에서 VLAN의 소속이 다른 노드들도 연결이 가능함을 볼 수 있다.

표6 MAC address VLAN 연결 결과표

S.A	D.A	종류	S1	S2	S3	S4
A1	A2	B	1	1		1
B3	C4	D				
A2	C1	D				
C3	C1	B	1		1	1
C2	A1	D				
B1	C3	D				
A2	A1	R		1		
A4	A3	B	1	1		1
C4	B3	D				1
A3	A4	R	1	1		1
B1	B4	B	1	1	1	1

표7 제안 알고리즘 적용연결 결과표

S.A	D.A	종류	S1	S2	S3	S4
A1	A2	B	1	1		1
B3	C4	B	1	1	1	1
A2	C1	R	1	1	1	
C3	C1	B	1		1	1
C2	A1	D				
B1	C3	B	1		1	1
A2	A1	R		1		
A4	A3	B	1	1		1
C4	A4	R				1
A3	A4	R	1	1		1
B1	B4	B	1	1	1	1

V. 결 론

본 연구는 고가의 Layer 3 스위치나 라우터를 사용하지 않고, Layer 2 스위치로 네트워크 구성의 탄력성을 높이기 위해 VLAN 범위를 동적으로 조절하는 알고리즘을 제안하였다. 이 알고리즘은 MAC address VLAN에서 FDB에 VID 연결 범위 테이블을 추가하고, C_VID 필드를 FDB에 추가하여 VLAN의 범위가 동적으로 조절되고 이를 통해 서로 다른 VLAN 사이의 통신 연결이 가능함을 보였다.

허브와 브리지는 통신전용 프로세서를 채택하여 지능적인 제어를 수행하고 있다. 따라서 본 논문의 제안 알고리즘을 프로세서의 루틴으로 내장하면 2계층에 적용 가능한 허브와 브리지를 설계할 수 있다.

참고문헌

[1] 조호형, LAN 상에서 VLAN의 적용에 관한 연구, pp 1-20, 1997

[2] David Passrmore and John Freeman, "The Virtual LAN Technology Report ", http://www.3com.com/nsc/200374.html, 1997

[3] Raj Jain, "Virtual LANs", http://www.cis.ohio-state.edu/~jain/cis788-97

[4] 조동호, 기가비트 이더넷 스위치를 위한 MAC 주소 검색 부의 설계, pp 17-28, 1998

[5] IEEE Standards 802.1Q, Virtual Bridged Local Area Networks